Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:

(a) providing an unprovisioned first packet-switched communications device in an enterprise network, the first packet-switched communications device having a corresponding unique identifier and an electronic address on the enterprise network;

(b) as part of [[the]]a provisioning process establishing, by the first packet-switched communications device, a secure communications session with a key generating agent in the enterprise network;

(c) providing, to the key generating agent through the session, (i) when a key identifier is derived using the unique identifier associated with the first packet-switched communications device, the unique identifier ~~associated with the communications device when a key identifier is derived using the unique identifier~~ or (ii) when the key identifier is derived using information not associated with the first packet-switched communications device, no unique identifier ~~when the key identifier is derived using information not associated with the communications device~~;

(d) receiving, from the key generating agent through the session, (i) a secret key derived from [[the]]an enterprise master key and a key identifier and (ii) the key identifier;

(e) forwarding to an application server a registration request, wherein the registration request ~~comprising~~comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first packet-switched communications device is successfully registered in step (g);

(f) authenticating the first packet-switched communications device with the secret key or an authentication key derived therefrom; and

(g) when the first packet-switched communications device is successfully authenticated, registering the first packet-switched communications device, wherein steps (b) through (e) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.

2. (Currently Amended) The method of Claim 1, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function and wherein the secret key is not in the possession of the first packet-switched communications device before step (d).

3. (Currently Amended) The method of Claim 1, wherein the electronic address is a telephone extension, wherein the first packet-switched communications device possesses [[a]]the secret key and the first packet-switched communications device is not in secure communications with the application server, and wherein the first packet-switched communications device provides [[a]]the registration request to the application server using the key identifier.

4. (Original) The method of Claim 1, further comprising before the establishing step:

authenticating the key generating agent;

performing the establishing, providing, and receiving steps when authenticating the key generating agent is successful.

5. (Currently Amended) The method of Claim 1, wherein the secret key is a symmetric key and wherein authentication step (f) is performed using symmetric key cryptography.

6. (Currently Amended) The method of Claim 1, wherein the secret key is derived from [[an]]the enterprise master key, the key identifier, and at least one of an attribute associated with the key generating agent and the unique identifier.

7. (Currently Amended) The method of Claim 6, wherein the enterprise master key is calculated using a seed value and a pseudorandom number generator, wherein the secret key is derived using the key generating agent attribute and unique identifier, wherein the attribute of key generating agent is an electronic address of the key generating agent and/or an electronic address of a server the key generating agent is resident on and wherein the unique identifier is the address of the first packet-switched communications device and/or a serial number associated with the first packet-switched communications device.

8. (Currently Amended) The method of Claim 1, wherein the ~~secret key is derived from an enterprise master key and the key identifier~~authentication key is used in authenticating step (f), wherein an integrity check value used in step (f) is a hashed message authentication code using the secret key, and wherein the authentication key is derived from the secret key of the first packet-switched communications device and an attribute of the first packet-switched communications device.

9. (Currently Amended) The method of Claim 1, wherein the key identifier computed from [[a]]the unique identifier comprises at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the first packet-switched communications device, and a counter field.

10. (Currently Amended) The method of Claim 9, wherein the unique identifier of the first packet-switched communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the first packet-switched

communications device on the enterprise network.

11. (Currently Amended) The method of Claim 1, further comprising:

digitally signing a message, wherein [[the]]a digital signature is derived from the secret key, a constant, and [[the]]a personal identification number of a user associated with the first packet-switched communications device.

12. (Currently Amended) The method of Claim 1, wherein ~~the receiving step further comprises receiving, from the key generating agent through the session, a key identifier~~a session pre-master secret is used, after step (g), by the first packet-switched communications device for establishing a secured session and wherein the pre-master secret is a function of the secret key, the unique identifier, a nonce value.

13. (Currently Amended) The method of Claim 1, ~~further comprising before~~ wherein the establishing step (b) comprises the sub-steps:

(B1) receiving [[an]]a first IP address assigned to the first packet-switched communications device and a second IP address assigned to an enterprise server comprising the key generating agent;

(B2) the first packet-switched communications device authenticating the enterprise server using public cryptography techniques;

(B3) the first packet-switched communications device generating a second secret key;

(B4) the first packet-switched communications device encrypting the second secret key with a public key associated with the enterprise server; and

(B5) the first packet-switched communications device sending the encrypted second secret key to the enterprise server.

14. (Original) The method of Claim 1, wherein the establishing step comprises:

establishing a logical connection with the key generating agent;

negotiating security parameters;

authenticating the identity of the key generating agent; and

when authentication is successful, activating the negotiated security parameters to establish the secured communications session.

15. (Original) The method of Claim 4, further comprising:

when authentication is successful, establishing secure communications.

16. (Currently Amended) The method of Claim 1, wherein the providing step comprises prompting a user associated with the first packet-switched communications device for a personal identification number and unique identifier.

17. (Currently Amended) The method of Claim 1, wherein the first packet-switched communications device provides to the key generating agent through the session, the key identifier when the first packet-switched communications device computes the key identifier.

18. (Original) The method of Claim 1, further comprising:

closing the secured session; and

computing a packet switched device authentication key using the secret key.

19. (Currently Amended) The method of Claim 1, wherein the step of authenticating further comprising:

when authentication is successful, establishing secure communication with the first packet-switched communications device.

20. (Currently Amended) A computer readable medium comprising processor executable instructions to perform the steps of Claim 1.

21. (Original) The method of Claim 1, wherein the establishing, providing and receiving steps are free of a challenge message and a response thereto.

22. (Original) A logic circuit operable to perform the steps of Claim 1.

23-62. (Canceled).

63. (New) An enterprise network including a first packet-switched communications device having a corresponding unique identifier and an electronic address on the enterprise network, the first packet-switched communications device comprising:

a first processor in the packet-switched communications device operable to:

(A1) establish, as part of a provisioning process, a secure communications session with a key generating agent in the enterprise network;

(A2) provide, to the key generating agent through the session, (i) when a key identifier is derived using a unique identifier associated with the first packet-switched communications device, the unique identifier or (ii) when the key identifier is derived using information not associated with the first packet-switched communications device, no unique identifier;

(A3) receive, from the key generating agent through the session, (i) a secret key derived from a key identifier and an enterprise master key and (ii) the key identifier;

(A4) forward to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first packet-switched communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first packet-

switched communications device is successfully registered in operation (B2); and wherein the application server comprises a second processor that is operable to:

(B1) authenticate the communications device with the secret key or an authentication key derived therefrom; and

(B2) when the communications device is successfully authenticated, register the communications device, wherein operations (A1) through (B1) occur after the first packet-switched communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.

64. (New) The enterprise network of Claim 63, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function and wherein the secret key is not in the possession of the first packet-switched communications device before operation (A3).

65. (New) The enterprise network of Claim 63, wherein the electronic address is a telephone extension, wherein the first packet-switched communications device possesses the secret key and the first packet-switched communications device is not in secure communications with the application server, and wherein the first packet-switched communications device provides the registration request to the application server using the key identifier.

66. (New) The enterprise network of Claim 63, further comprising, before the establishing operation (A1), the sub-operations of:

(i) authenticating the key generating agent;

(ii) performing the establishing, providing, and receiving operations when authenticating the key generating agent is successful.

67. (New) The enterprise network of Claim 63, wherein the secret key is a symmetric key and wherein authentication operation (B1) is performed using symmetric key cryptography.

68. (New) The enterprise network of Claim 63, wherein the secret key is derived from the enterprise master key, the key identifier, and at least one of an attribute associated with the key generating agent and the unique identifier.

69. (New) The enterprise network of Claim 68, wherein the enterprise master key is calculated using a seed value and a pseudo-random number generator, wherein the secret key is derived using the key generating agent attribute and unique identifier, wherein the attribute of key generating agent is an electronic address of the key generating agent and/or an electronic address of a server the key generating agent is resident on and wherein the unique identifier is the address of the first packet-switched communications device and/or a serial number associated with the first packet-switched communications device.

70. (New) The enterprise network of Claim 63, wherein the authentication key is used in authenticating operation (B1), wherein an integrity check value used in operation (B1) is a hashed message authentication code using the secret key, and wherein the authentication key is derived from the secret key of the first packet-switched communications device and an attribute of the first packet-switched communications device.

71. (New) The enterprise network of Claim 63, wherein the key identifier computed from the unique identifier comprises at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the communications device, and a counter field.

72. (New) The enterprise network of Claim 71, wherein the unique identifier of the first packet-switched communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the first packet-switched communications device on the enterprise network.

73. (New) The enterprise network of Claim 63, further comprising the operation of:

digitally signing a message, wherein a digital signature is derived from the secret key, a constant, and a personal identification number of a user associated with the first packet-switched communications device.

74. (New) The enterprise network of Claim 63, wherein a session pre-master secret is used, after operation (B2), by the first packet-switched communications device for establishing a secured session and wherein the pre-master secret is a function of the secret key, the unique identifier, a nonce value.

75. (New) The enterprise network of Claim 63, wherein the establishing operation (A1) comprises the sub-operations:

(A1i) receiving a first IP address assigned to the first packet-switched communications device and a second IP address assigned to the application server comprising the key generating agent;

(A1ii) the first packet-switched communications device authenticating the application server using public cryptography techniques;

(A1iii) the first packet-switched communications device generating a second secret key;

(A1iv) the first packet-switched communications device encrypting the second secret key with a public key associated with the application server; and

(A1v) the first packet-switched communications device sending the encrypted

second secret key to the application server.

76. (New) The enterprise network of Claim 63, wherein the establishing operation (A1) comprises the sub-operations:

establishing a logical connection with the key generating agent;

negotiating security parameters;

authenticating the identity of the key generating agent; and

when authentication is successful, activating the negotiated security parameters to establish the secured communications session.

77. (New) The enterprise network of Claim 66, further comprising the operation by the second processor of:

(B3) when authentication is successful, establishing secure communications.

78. (New) The enterprise network of Claim 63, wherein the a user associated with the first packet-switched communications device is prompted by the processor for a personal identification number and unique identifier.

79. (New) The enterprise network of Claim 63, wherein the first packet-switched communications device provides to the key generating agent through the session, the key identifier when the first packet-switched communications device computes the key identifier.

80. (New) The enterprise network of Claim 63, further comprising the operations of:

closing the secured session; and

computing a packet switched device authentication key using the secret key.

81. (New) The enterprise network of Claim 63, wherein the authentication operation (B1) comprises the sub-operation of:

when authentication is successful, establishing secure communication with the communications device.

82. (New) A method for provisioning and registering a packet-switched communications device in an enterprise network, comprising:

(a) assigning an electronic address to a first communications device;

(b) providing the electronic address and an address associated with a key generating agent to the first communications device;

(c) authenticating, by the first communications device, the key generating agent; and

(d) when authentication of the key generating agent is successful, performing the following additional steps:

(e) establishing, as part of a provisioning process, a secure communications session between the first communications device and the key generating agent, wherein the first communications device has a corresponding unique identifier;

(f) providing the unique identifier to the key generating agent through the secure communications session;

(g) receiving, from the key generating agent through the session, (i) a secret key derived from an enterprise master key, the unique identifier, and a key identifier and (ii) the key identifier;

(h) forwarding to an application server a registration request, wherein the registration request comprises the key identifier and wherein the first communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first communications device is successfully registered in step (j);

(i) authenticating the first communications device with the secret key or an authentication

key derived therefrom; and

(j) when the first communications device is successfully authenticated, registering the first communications device, wherein steps (e) through (j) occur after the first communications device has been located at an end user's premises and wherein the first and second packet-switched communications device have different and unique secret keys and key identifiers.

83. (New) The method of Claim 82, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function and wherein the secret key is not in the possession of the first communications device before step (g).

84. (New) The method of Claim 82, wherein the electronic address is a telephone extension, wherein the first communications device possesses the secret key and the first communications device is not in secure communications with the application server, and wherein the first communications device provides the registration request to the application server using the key identifier.

85. (New) The method of Claim 82, wherein the secret key is a symmetric key and wherein authentication step (i) is performed using symmetric key cryptography.

86. (New) The method of Claim 82, wherein the secret key is derived from the enterprise master key, the key identifier, and at least one of an attribute associated with the key generating agent and the unique identifier.

87. (New) The method of Claim 85, wherein the enterprise master key is calculated using a seed value and a pseudo-random number generator, wherein the secret key is derived using the key generating agent attribute and unique identifier, wherein the attribute of key

generating agent is an electronic address of the key generating agent and/or an electronic address associated with the key generating agent, and wherein the unique identifier is the address of the first communications device and/or a serial number associated with the first communications device.

88. (New) The method of Claim 82, wherein the authentication key is used in authenticating step (i), wherein an integrity check value used in step (i) is a hashed message authentication code using the secret key, and wherein the authentication key is derived from the secret key of the first communications device and an attribute of the first communications device.

89. (New) The method of Claim 82, wherein the key identifier computed from the unique identifier comprises at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the identifier of the first communications device, and a counter field.

90. (New) The method of Claim 89, wherein the unique identifier of the first communications device is at least one of an extension on the enterprise network, a serial number, a user login identifier, and an address of the first communications device on the enterprise network.

91. (New) The method of Claim 82, further comprising:

(k) digitally signing a message, wherein a digital signature is derived from the secret key, a constant, and a personal identification number of a user associated with the first communications device.

92. (New) The method of Claim 82, wherein a session pre-master secret is used, after step (g), by the first communications device for establishing a secured session and wherein the pre-master secret is a function of the secret key, the unique identifier, a nonce value.

93. (New) The method of Claim 82, wherein the establishing step (e) comprises the sub-steps:

(E1) receiving a first IP address assigned to the first communications device and a second IP address assigned to an enterprise server comprising the key generating agent;

(E2) the first communications device authenticating the enterprise server using public cryptography techniques;

(E3) the first communications device generating a second secret key;

(E4) the first communications device encrypting the second secret key with a public key associated with the enterprise server; and

(E5) the first communications device sending the encrypted second secret key to the enterprise server.

94. (New) The method of Claim 82, wherein the establishing step (e) comprises:

(E1) establishing a logical connection with the key generating agent;

(E2) negotiating security parameters;

(E3) authenticating the identity of the key generating agent; and

(E4) when authentication is successful, activating the negotiated security parameters to establish the secured communications session.

95. (New) The method of Claim 82, wherein the providing step comprises prompting a user associated with the first communications device for a personal identification number and unique identifier.

96. (New) The method of Claim 82, wherein the first communications device provides to the key generating agent through the session, the key identifier when the first communications device computes the key identifier.

97. (New) The method of Claim 82, further comprising:

(k) closing the secured session; and

(l) computing a packet switched device authentication key using the secret key and wherein the step of authenticating further comprising:

when authentication is successful, establishing secure communication with the first communications device.

98. (New) A computer readable medium comprising processor executable instructions to perform the steps of Claim 82.

99. (New) A method, comprising:

(a) requesting, by an unprovisioned and unregistered first communications device, a first electronic address to be assigned to the first communications device and a second electronic address associated with a key generating agent;

(b) receiving, by the first communication device, the first and second electronic addresses;

(c) thereafter contacting and authenticating, by the first communications device, the key generating agent;

(d) when authentication of the key generating agent is successful, establishing, by the first communications device and as part of a provisioning process, a secure communications session with the key generating agent, wherein the first communications device has a corresponding unique identifier;

(e) providing the unique identifier to the key generating agent through the secure

communications session;

(g) receiving, from the key generating agent through the session, a secret key derived from an enterprise master key, the unique identifier, and a key identifier;

(h) forwarding, to an application server, a registration request, wherein the registration request comprises the key identifier and wherein the unregistered first communications device has a limited ability to communicate with a provisioned and registered second packet-switched communications device in the enterprise network until the first communications device is successfully registered; and

(i) when the application server, has successfully authenticated the first communications device using the secret key or an authentication key derived therefrom, registering the first communications device, wherein steps (a) through (i) occur after the first communications device has been located at an end user's premises and wherein the first and second packet-switched communications devices have different and unique secret keys and key identifiers.

100. (New) The method of Claim 99, wherein the key identifier is a function of at least one of a psuedo-random number generator, a database of keys and key identifiers, and a hash function, wherein the secret key is not in the possession of the first communications device before step (g), wherein the electronic address is a telephone extension, wherein the secret key is a symmetric key, wherein authentication of the first communication device is performed by the application server using symmetric key cryptography, wherein the enterprise master key is calculated using a seed value and a pseudo-random number generator, wherein the secret key is derived using a key generating agent attribute and unique identifier, wherein the unique identifier is the first electronic address of the first communications device and/or a serial number associated with the first communications device, wherein the authentication key and integrity check value are used by the application server in authenticating the first communications device, wherein the integrity check value is a hashed message authentication code using the secret key, wherein the authentication key is derived from the secret key of the first communications device

and an attribute of the first communications device, and wherein the key identifier computed from the unique identifier comprises at least a first field, the first field comprising an identifier associated with the key generating agent, a second field comprising the unique identifier of the first communications device, and a counter field.

101. (New) The method of Claim 99, wherein step (c) comprises the sub-steps:

(C1) the first communications device authenticating the application server using public cryptography techniques;

(C2) the first communications device generating a second secret key;

(C3) the first communications device encrypting the second secret key with a public key associated with the application server; and

(C4) the first communications device sending the encrypted second secret key to the application server.

102. (New) A computer readable medium comprising processor executable instructions to perform the steps of Claim 99.